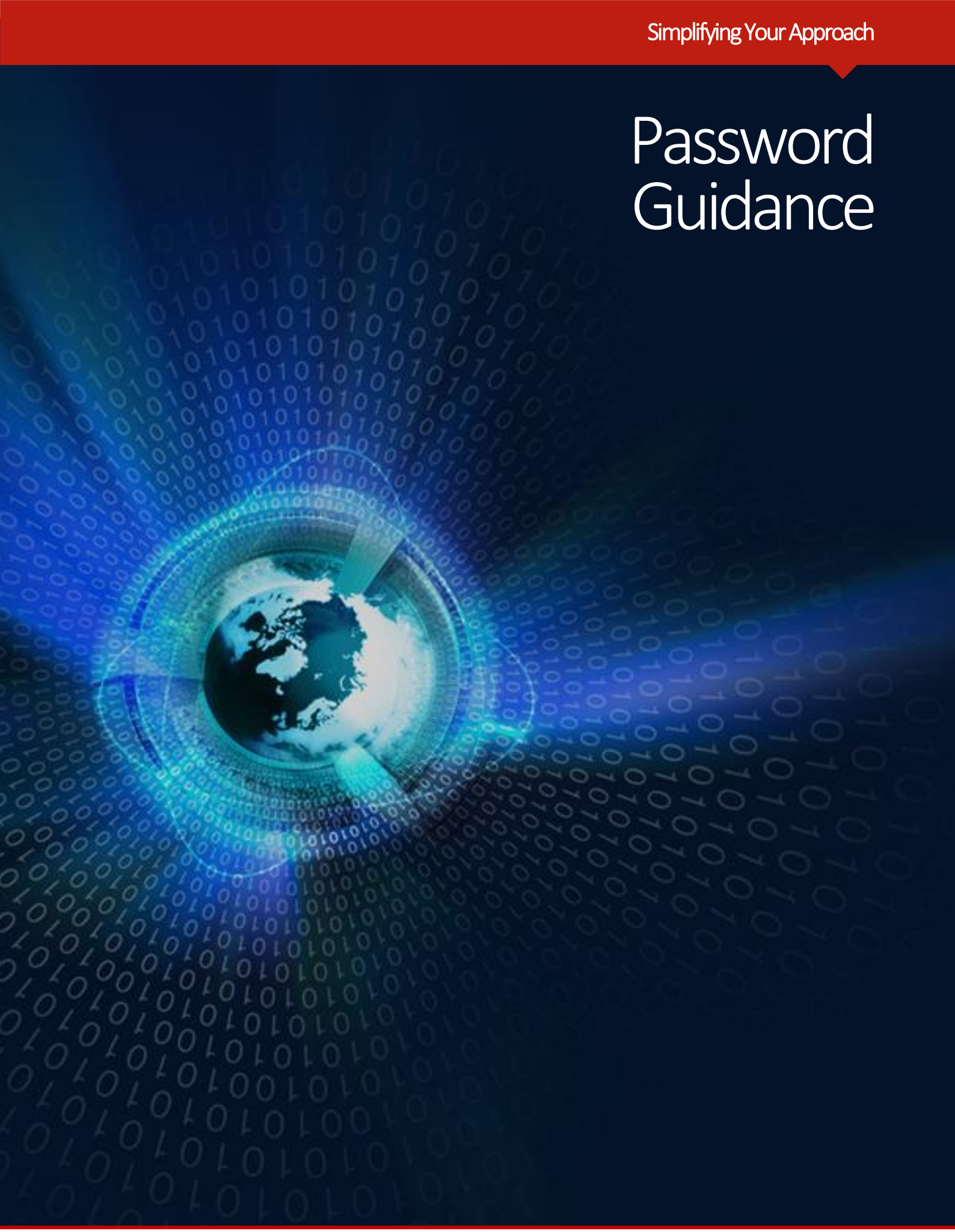
Simplifying Your Approach

Password Guidance



CESG
The Information Security Arm of GCHQ

CPNI
Centre for the Protection of National Infrastructure

Contents

Foreword

Passwords are an essential part of modern life. Every day we provide passwords as authentication to systems and services, both in the workplace and at home. A recent survey reported that UK citizens each had an average of 22 online passwords[1], far more than most people can easily remember.

Password guidance - including previous CESG guidance - has encouraged system owners to adopt the approach that complex passwords are 'stronger'. The abundance of sites and services that require passwords means users have to follow an impossible set of password rules in order to 'stay secure'.

Worse still, the rules - even if followed - don't necessarily make your system more secure. Complex passwords do not usually frustrate attackers, yet they make daily life much harder for users. They create cost, cause delays, and may force users to adopt workarounds or non-secure alternatives that increase risk.

"By simplifying your organisation's approach to passwords, you can reduce the workload on users, lessen the support burden on IT departments, and combat the false sense of security that unnecessarily complex passwords can encourage."

Password Guidance: Simplifying Your Approach contains advice for system owners responsible for determining password policy. It is not intended to protect high value individuals using public services. It advocates a dramatic simplification of the current approach at a **system** level, rather than asking **users** to recall unnecessarily complicated passwords.

More specifically, this document will help you to:

- examine and (if necessary) challenge existing corporate password policies, and argue for a more realistic approach
- understand the decisions to be made when determining password policy
- implement strategies that lessen the workload that complex passwords impose on users
- make your system more secure by suggesting a number of practical steps you can implement

Every single user in the UK public sector has at least one (and most likely considerably more) work-related password. By simplifying your organisation's approach, you can reduce the workload on users, lessen the support burden on IT departments, and combat the false sense of security that unnecessarily complex passwords can encourage.

Ciaran Martin

Director General for Cyber Security, GCHQ

Introduction: the problems with passwords

The death of the password was predicted some ten years ago. It was assumed that alternative authentication methods would be adopted to control access to IT infrastructure, data, and user material. But since then, password use has only risen.

This increase in password use is mostly due to the surge of online services, including those provided by government and the wider public sector. Passwords are an easily-implemented, low-cost security measure, with obvious attractions for managers within enterprise systems. However, this proliferation of password use, and increasingly complex password requirements, places an unrealistic demand on most users.

Inevitably, users will devise their own coping mechanisms to cope with 'password overload'. This includes writing down passwords, re-using the same password across different systems, or using simple and predictable password creation strategies. A study within a Scottish NHS trust found that 63% of its users admitted to re-using passwords.[2]

How are passwords discovered?

Attackers use a variety of techniques to discover passwords. Many of these techniques are freely available and documented on the Internet, and use powerful, automated tools.

[2] 'Blaming Noncompliance Is Too Convenient: What Really Causes Information Breaches', Security & Privacy, IEEE (Volume: 10, Issue; 3)

Approaches to discovering passwords include:

- social engineering eg phishing; coercion
- manual password guessing, perhaps using personal information 'cribs' such as name, date of birth, or pet names
- intercepting a password as it is transmitted over a network
- 'shoulder surfing', observing someone typing in their password at their desk
- installing a keylogger to intercept passwords when they are entered into a device
- searching an enterprise's IT infrastructure for electronically stored password information
- brute-force attacks; the automated guessing of large numbers of passwords until the correct one is found
- finding passwords which have been stored insecurely, such as handwritten on paper and hidden close to a device
- compromising databases containing large numbers of user passwords, then using this information to attack other systems where users have re-used these passwords

About this document

The remaining sections in this document comprise 7 tips that summarise the key areas to consider when defining password policy. Each section also contains practical steps you can implement to optimise system security.

Tip 1: Change all default passwords

Factory-set default passwords being left unchanged is one of the most common password mistakes that organisations make.

By leaving default credentials in place, networking and crucial infrastructure is reachable online. In 2012, the 'Carna Internet Census' found "several hundred thousand unprotected devices on the Internet". The Carna botnet commandeered these devices with default passwords to create a temporary research botnet[3].

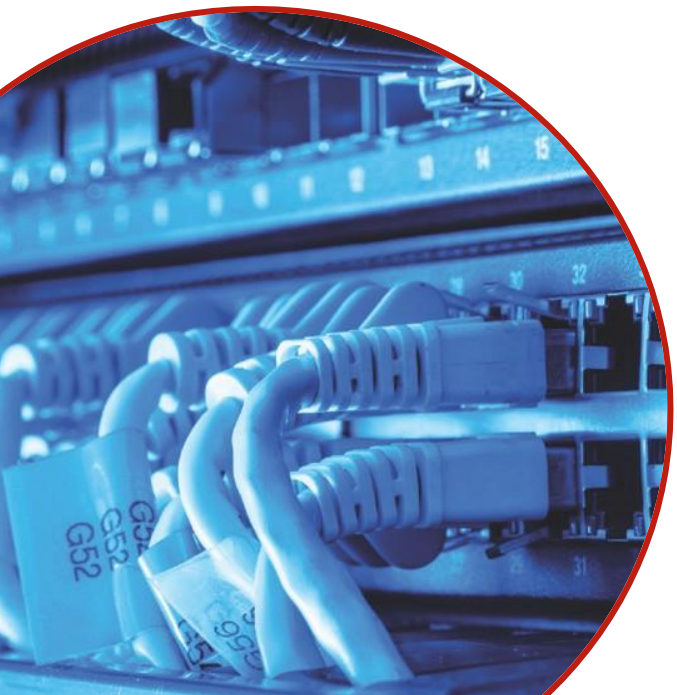
All default vendor-supplied passwords that come with any system or software should be changed before deployment. Pay particular attention to essential infrastructure devices such as routers, wireless access points, and firewalls.

Vendors can help here by documenting all default passwords, and listing how to change them.

In summary

- Change all default passwords before deployment.
- Carry out a regular check of system devices and software, specifically to look for unchanged default passwords.
- Prioritise essential infrastructure devices.

[3] http://internetcensus2012.bitbucket.org/paper.html



Tip 2: Help users cope with password overload

Users are generally told to remember passwords, and to not share them, re-use them, or write them down. But the typical user has dozens of passwords to remember – not just yours.

An important way to minimise the password burden is to only implement passwords when they are really needed. Systems and services with no security requirements should be free from password control. Technical solutions (such as single sign-on and password synchronisation) can also reduce the burden on staff. These may incur additional costs, but this is outweighed by the benefits they bring to the whole system security.

You should also provide appropriate facilities to store recorded passwords, with protection appropriate to the sensitivity of the information being secured. Storage could be physical (for example secure cabinets) or technical (such as password management software), or a combination of both. The important thing is that your organisation provides a *sanctioned mechanism* to help users manage passwords, as this will deter users from adopting insecure 'hidden' methods to manage password overload.

Password management software

Software password managers can help users by generating, storing and even inputting passwords when required. However, like any piece of security software, they are not impregnable and are an attractive target for attackers.

Changing passwords

Most administrators will force users to change their password at regular intervals, typically every 30, 60 or 90 days. This imposes burdens on the user (who is likely to choose new passwords that are only minor variations of the old) and carries no real benefits as stolen passwords are generally exploited immediately. Long-term illicit use of compromised passwords is better combated by:

- monitoring logins to detect unusual use
- notifying users with details of attempted logins, successful or unsuccessful; they should report any for which they were not responsible

Regular password changing harms rather than improves security, so avoid placing this burden on users. However, users must change their passwords on indication or suspicion of compromise.

Sharing passwords

You should never allow password sharing between users. Sharing accounts, or even occasional use by anyone other than the account holder, negates the benefit of authenticating a specific user. In particular, the ability to audit and monitor a specific user's actions is lost.

Where password sharing is currently in use (for example, where emergency access is required to access patient medical records in A&E/critical care units), you should consider alternative access control mechanisms such as the presentation of a hardware token, such as an RFID badge.

In summary

- Users have a whole suite of passwords to manage, not just yours.
- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication or suspicion of compromise.
- Allow users to reset passwords easily, quickly and cheaply.
- Do not allow password sharing.
- Password management software can help users, but carries risks.

Tip 3: Understand the limitations of user-generated passwords

User-generated password schemes are more commonly used than machine-generated ones, due to being simpler, cheaper and quicker to implement. However, user-generated password schemes carry risks that machine-generated schemes do not.

Studies of user-generated password schemes have shown that they encourage insecure behaviours. These include using the most common passwords, re-using the same password over multiple systems, and adopting predictable password generation strategies (such as replacing the letter 'o' with a zero).

Attackers are familiar with these strategies and use this knowledge to optimise their attacks. Most dictionaries for brute-force attacks will prioritise frequently used words and character substitutions. This means that systems with user-generated passwords will normally contain a large number of weak passwords that will quickly fall to an automated guessing attack.

Technical controls vs complex passwords

Traditionally, organisations impose rules on the length and complexity of passwords. However, people then tend to use predictable strategies to generate passwords, so the security benefit is marginal while the user burden is high.

The use of technical controls to defend against automated guessing attacks is far more effective than relying on users to generate (and remember) complex passwords.

For this reason, enforcing the requirement for complex character sets in passwords is not recommended. Instead, concentrate efforts on technical controls, especially:

- defending against automated guessing attacks by either using account lockout, throttling, or protective monitoring (as described in Tip 6)
- blacklisting the most common password choices

Similarly, given the infeasibility of memorising multiple passwords, many are likely to be re-used. Users should only do this where the compromise of one password does not result in the compromise of more valuable data protected by the same password on a different system. One golden rule is users should never use the same password for both home and work.

Reinforce password policy with staff training that helps users to avoid creating passwords that are easy-to-guess. Training can advise that passwords should avoid personal information (names, dates, sports teams, etc.), simple dictionary words or predictable keyboard sequences.

Password strength meters

Password strength meters aim to help users assess the strength of their self-generated passwords. They may steer users away from the weakest passwords, but often fail to account for the factors that can make passwords weak (such as using personal information, and repeating characters or common character strings).

In summary

- Put technical defences in place so that simpler password policies can be used.
- Reinforce policies with good user training. Steer users away from choosing predictable passwords, and prohibit the most common ones by blacklisting.
- Tell users that work passwords protect important assets; they should never re-use passwords between work and home.
- Be aware of the limitations of password strength meters.

Tip 4: Understand the limitations of machine-generated passwords

Machine-generated passwords eliminate those passwords that would be simple for an attacker to guess. They require little effort from the user to create, and, depending on the generation scheme, can produce passwords that are fairly easy to remember.

The main advantage of machine-generated schemes is that they eliminate those passwords that would be simple for an attacker to guess. They also deliver a known level of 'randomness' so it's possible to calculate the time it would take to crack the password using a brute-force attack.

Compared to user-generated schemes, there is no need to use blacklisting, and user training should be simpler. They also require little effort from the user for password creation.

Some machine generation schemes can produce passwords which are very difficult for people to remember. This increases both the demand on helpdesk for resets, and also the likelihood of insecure storage. They are not recommended.

Instead, use a generation scheme designed for high memorability (such as passphrases, 4 random dictionary words or CVC-CVC-CVC[4] style passwords). Ideally, you should give users a choice of passwords, so they can select the one they find the most memorable.

Technical controls

Technical controls such as account lockout, throttling or protective monitoring are still relevant when using machine-generated passwords.

In summary

- Choose a scheme that produces passwords that are easier to remember.
- Offer a choice of passwords, so users can select one they find memorable.
- As with user-generated passwords, tell users that work passwords protect important assets; they should never re-use passwords between work and home.

[4] Consonant-vowel-consonant constructions

Tip 5: Prioritise administrator and remote user accounts

Administrator accounts have highly privileged access to systems and services. Compromise of these accounts is a threat to the wider system, and therefore especially attractive to attackers.

Ensure that robust measures are in place to protect administrator accounts. Administrator accounts should not be used for high risk or day-to-day user activities, such as accessing external email or browsing the Internet. Administrators should also have 'standard' user accounts for normal business use (with different passwords).

Remote users

Remote users who require remote login access, which can include the use of VPNs, email/webmail and other forms of access to internal systems, should be required to provide extra evidence (such as a token). This can form part of your two factor authentication policy for all remote accounts.

In summary

- Give administrators, remote users and mobile devices extra protection.
- Administrators must use different passwords for their administrative and non-administrative accounts.
- Do not routinely grant administrator privileges to standard users.
- Consider implementing two factor authentication for all remote accounts.
- Make sure that absolutely no default administrator passwords are used.

Tip 6: Use account lockout and protective monitoring

Account lockout, throttling, and protective monitoring are powerful defences against brute-force attacks on enterprise systems and online services.

Password systems can be configured so that a user only has a limited number of attempts to enter their password before their account is locked out. Or, the system can add a time delay between successive login attempts - a technique known as 'throttling'.

Account lockout is simpler to implement than throttling, but can have a detrimental impact on the user experience. Account lockout also provides an attacker with an easy way to launch a denial of service attack, particularly for large scale online systems.

If using lockout, we recommend you allow around 10 login attempts before the account is frozen. This gives a good balance between security and usability[5].

Protective monitoring

The burden of locking out legitimate user accounts can be relaxed if other approaches to detecting and preventing the misuse of accounts are considered. For example, you can use protective monitoring to detect and alert to malicious or abnormal behaviour, such as automated attempts to guess or brute-force account passwords.

Password blacklisting

For user generated password schemes, a helpful defence is to employ a password blacklist to disallow the most common password choices. This works well in combination with other defences by reducing the chance that a small number of guesses will break a password.

Outsourcing and the use of third parties

When services are outsourced, you should provide the third party with instructions that clearly describe the measures they should take to protect the credentials used to access systems or data relating to the issuing organisation. This should form part of the contractual agreement.

In summary

- Account lockout and 'throttling' are effective methods of defending brute-force attacks.
- Allow users around 10 login attempts before locking out accounts.
- Password blacklisting works well in combination with lockout or throttling.
- Protective monitoring is also a powerful defence against brute-force attacks, and offers a good alternative to account lockout or throttling.
- When outsourcing, contractual agreements should stipulate how user credentials are protected.

[5] 'Ten strikes and you're out: increasing the number of login attempts can improve password usability', Brostoff and Sasse, CHI Workshop 2003

Tip 7: Don't store passwords as plain text

Passwords should never be stored as plain text, even if the information on the protected system is relatively unimportant. This section gives advice for system developers and engineers, and will help security practitioners select products that provide more secure methods of password storage and processing.

We've read how users re-use passwords and employ predictable password creation strategies. This means an attacker who gains access to a database containing plain text passwords already knows a user's credentials for one system. They can use this information to attempt to access more important accounts, where further damage can be done.

Periodically search systems for password information that is stored in plain text. Consider establishing automated processes that (for example) regularly search for clear text emails and documents containing the word 'password' in the filename or body.

If you need to provide access to clear text passwords (such as when a selection of characters are requested during a login), use an alternative method of protection (for example, on-demand decryption).

Hashing and salting

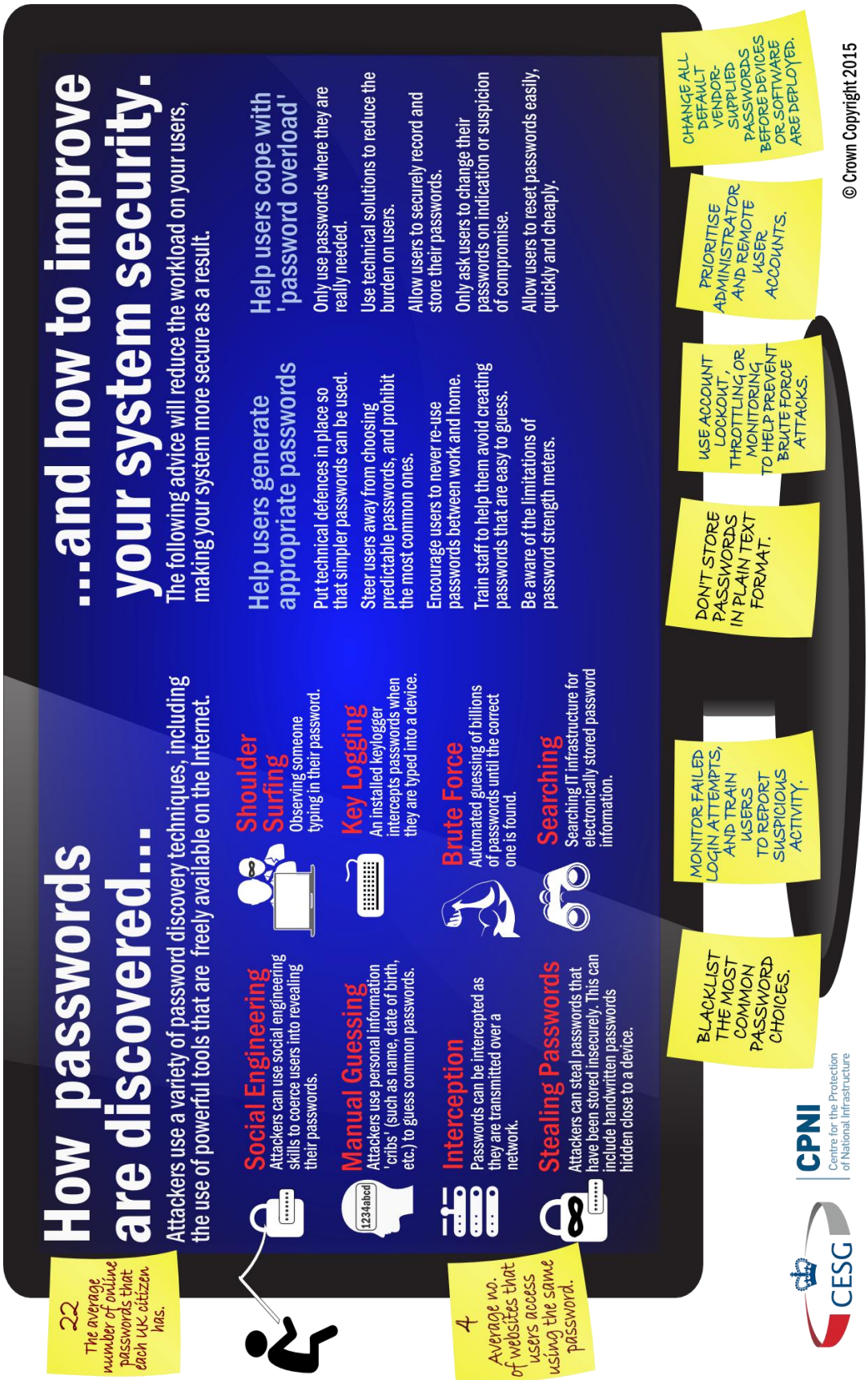
Hashing is a one-way cryptographic function which converts a plain text password into a 'hash'. An attacker who has accessed a database containing password hashes will not know the actual passwords.

However, attackers can still use brute-force attacks and rainbow tables (pre-computed tables for reversing cryptographic hash functions) to retrieve passwords from stolen hashes. For this reason, a 'salt' should be added to the password before hashing.

In summary

- Never store passwords as plain text.
- Produce hashed representations of passwords using a unique salt for each account.
- Store passwords in a hashed format, produced using a cryptographic function capable of multiple iterations (such as SHA 256).
- Ensure you protect files containing encrypted or hashed passwords from unauthorised system or user access.
- When implementing password solutions use public standards, such as PBKDF2, which use multiple iterated hashes.

Infographic summary



Disclaimer

This document has been produced jointly by GCHQ and CPNI. It is not intended to be an exhaustive guide to potential cyber threats, is not tailored to individual needs and is not a replacement for specialist advice. Users should ensure they take appropriate specialist advice where necessary.

This document is provided without any warranty or representation of any kind whether express or implied. The government departments involved in the production of this document cannot therefore accept any liability whatsoever for any loss or damage suffered or costs incurred by any person arising from the use of this document.

Findings and recommendations in this document have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risks. Ownership of information risks remains with the relevant system owner at all times.

CESG

The Information Security Arm of GCHQ

CPNI

Centre for the Protection of National Infrastructure